AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1-29. (Cancelled)

30. (Currently Amended) A method for retrieving a value secured in a key management system comprising:

receiving a request for the value secured in the key management system;

retrieving a serialized file from a key management system storage;

de-serializing the serialized file producing a de-serialized file;

decoding an encoded key list in the de-serialized file to produce a decoded key list;

searching for a key corresponding to the value in the decoded key list;

inputting a key encryption key into the key management system;

hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file;

comparing the key encryption key hash to [[a]] the hashed key encryption key in the de-serialized file to grant access to the key management system;

decrypting a secret token in the de-serialized file using the key encryption key ~~if the key encryption key hash is equal to the hashed key encryption key in the de-serialized file~~ to produce at least one tuple after access to the key management system is granted;

storing the at least one tuple in a data structure within the key management system; and

retrieving [[the]] a tuple corresponding to the value from the at least one tuple, [[if]] using the key corresponding to the value ~~is in the decoded key list~~.

31. (Currently Amended) The method of claim 30, further comprising:

searching a local file system~~, if the key corresponding to the value~~ for the key when the key is not found in the decoded key list.

32. (Currently Amended) A method for changing an existing key encryption key, comprising:

entering the existing key encryption key;

entering a new key encryption key;

de-serializing a serialized file producing a de-serialized file;

hashing the existing key encryption key producing a hashed key encryption key, wherein the hashed key encryption key is equal to a key encryption key hash in the de-serialized file;

comparing the hashed key encryption key to [[a]] the key encryption key hash in the de-serialized file to grant access to a key management system;

decrypting a secret token using the existing key encryption key ~~if the hashed key encryption key equals the key encryption key hash producing~~ to produce a tuple after access to the key management system is granted;

encrypting the tuple using the new key encryption key producing a new secret token;

hashing the new key encryption key producing a new hashed key encryption key; and

serializing the new hashed key encryption key and the new secret token to produce a new serialized file.

33. (Cancelled)

34. (Currently Amended) An apparatus for retrieving a value secured in a key management system comprising:

means for receiving a request for the value secured in the key management system;

means for retrieving a serialized file from a key management system storage;

means for de-serializing the serialized file producing a de-serialized file;

means for decoding an encoded key list in the de-serialized file to produce a decoded key list;

means for searching for a key corresponding to the value in the decoded key list;

means for inputting a key encryption key into the key management system;

means for hashing the key encryption key to produce a key encryption key hash, wherein the key encryption key hash is equal to a hashed key encryption key in the de-serialized file;

means for comparing the key encryption key hash to [[a]] the hashed key encryption key in the de-serialized file to grant access to the key management system;

means for decrypting a secret token in the de-serialized file using the key encryption key ~~if the key encryption key hash is equal to the hashed key encryption key in the de-serialized file~~ to produce at least one tuple after access to the key management system is granted;

means for storing the at least one tuple in a data structure within the key management system; and

means for retrieving [[the]] a tuple corresponding to the value from the at least one tuple, [[if]] using the key corresponding to the value ~~is in the decoded key list~~.

35. (Currently Amended) An apparatus for changing an existing key encryption key, comprising:

means for entering the existing key encryption key;

means for entering a new key encryption key;

means for de-serializing a serialized file producing a de-serialized file;

means for hashing the existing key encryption key producing a hashed key encryption key, wherein the hashed key encryption key is equal to a key encryption key hash in the de-serialized file;

means for comparing the hashed key encryption key to [[a]] the key encryption key hash in the de-serialized file to grant access to a key management system;

means for decrypting a secret token using the existing key encryption key ~~if the hashed key encryption key equals the key encryption key hash producing~~ to produce a tuple after access to the key management system is granted;

means for encrypting the tuple using the new key encryption key producing a new secret token;

means for hashing the new key encryption key producing a new hashed key encryption key; and

means for serializing the new hashed key encryption key and the new secret token to produce a new serialized file.

36-38. (Cancelled)